Man-in-the-Middle Attacks without Rogue AP: When WPAs Meet ICMP Redirects

Xuewei Feng[1)], Qi Li[1,3)], Kun Sun[2)], **Yuxiang Yang**[1)], Ke Xu[1,3)]

1) Tsinghua University & BNRist

2) George Mason University

3) Zhongguancun Lab

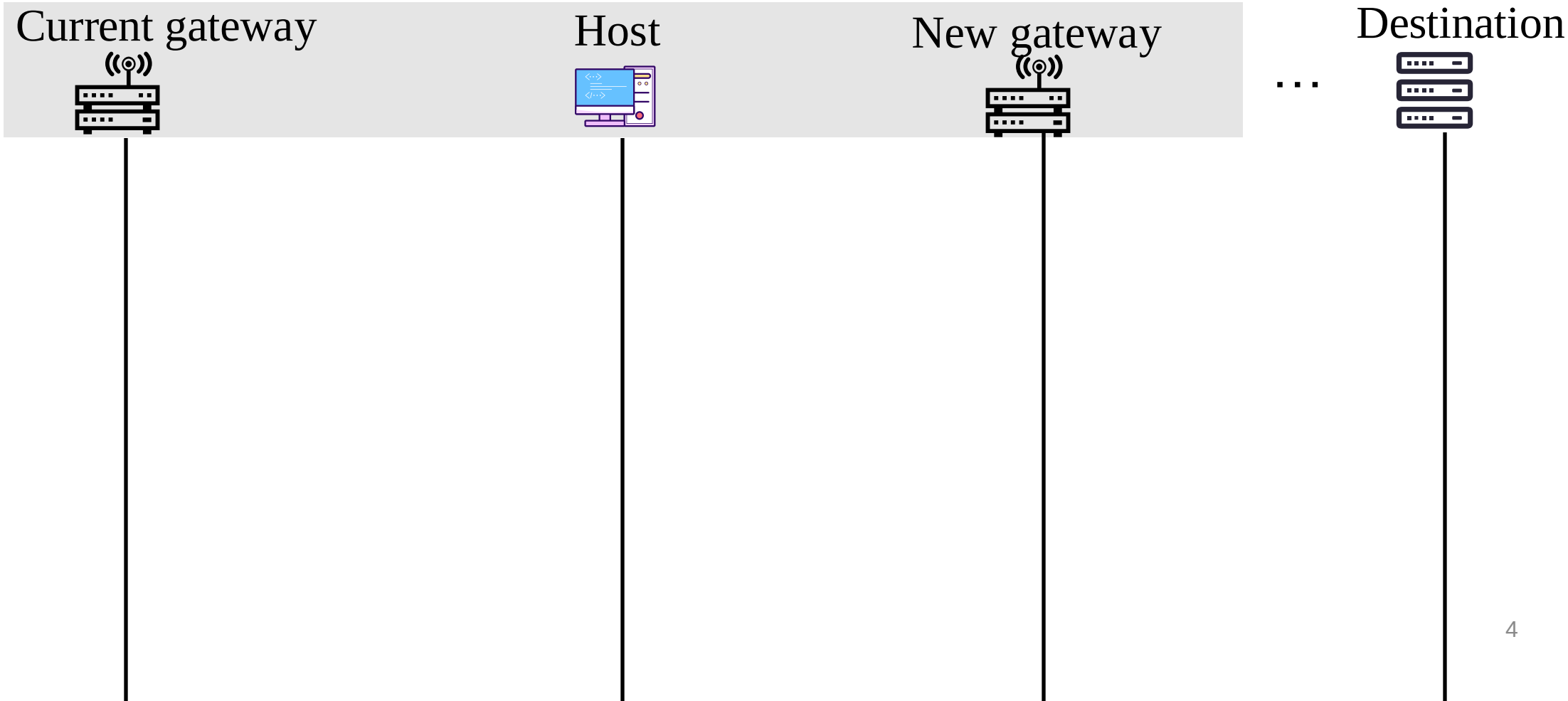
Overview

- The Mechanism of ICMP Redirect
- Legitimacy Check over ICMP Redirects
- Traffic Hijacking in Wi-Fi Networks
- Empirical Study
- Countermeasures
- Conclusion

The Mechanism of ICMP Redirect

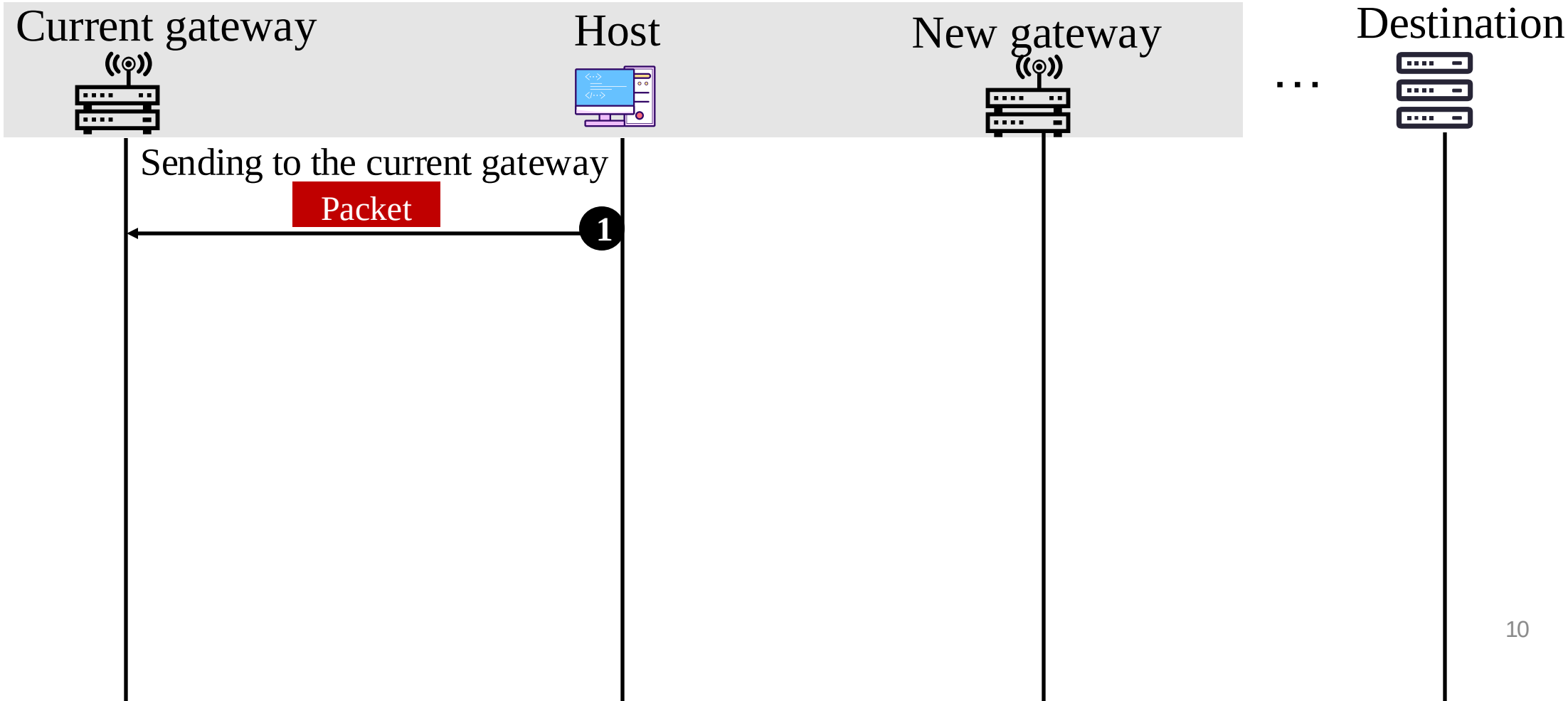
The Mechanism of ICMP Redirect

ICMP redirects help Host update its routing and optimize the forwarding path dynamically, thus improving the network performance.



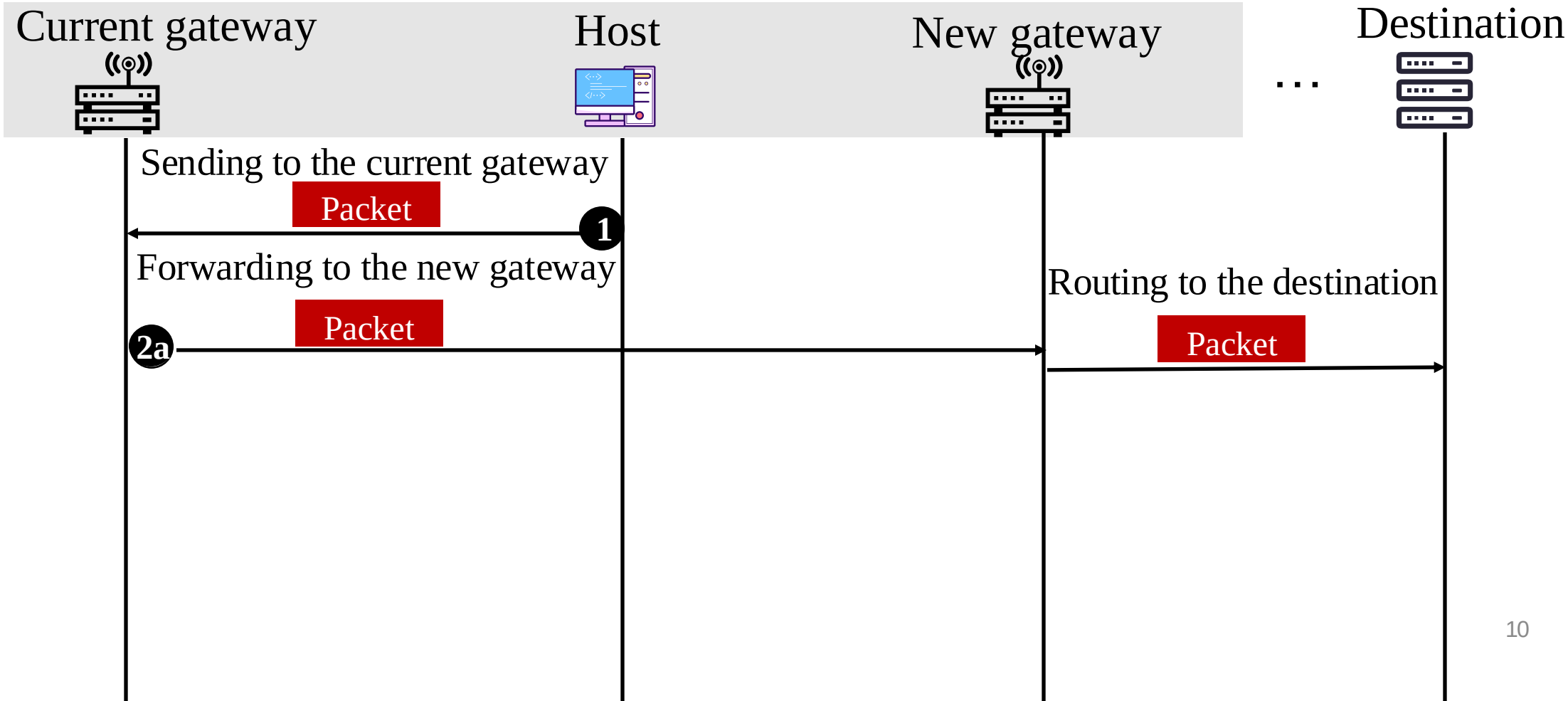
The Mechanism of ICMP Redirect

ICMP redirects help Host update its routing and optimize the forwarding path dynamically, thus improving the network performance.



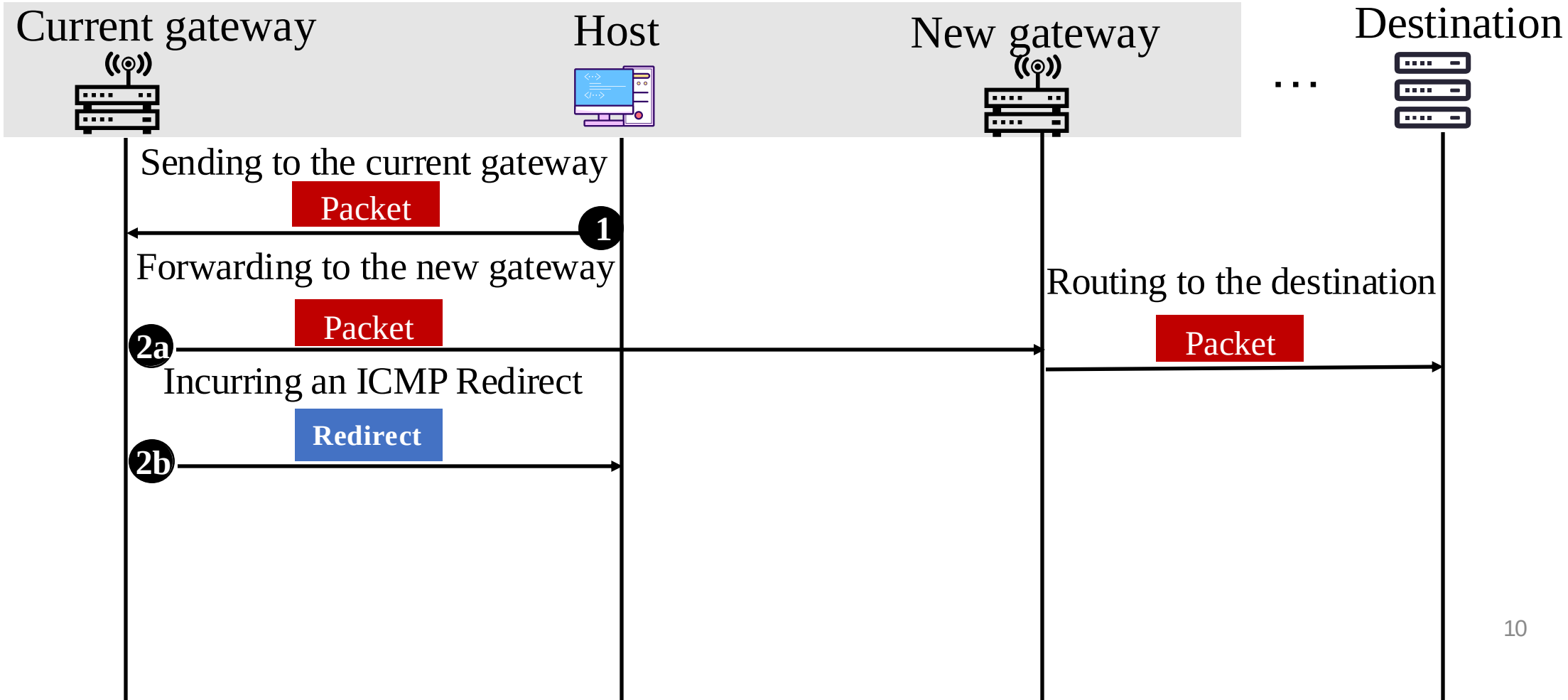
The Mechanism of ICMP Redirect

ICMP redirects help Host update its routing and optimize the forwarding path dynamically, thus improving the network performance.



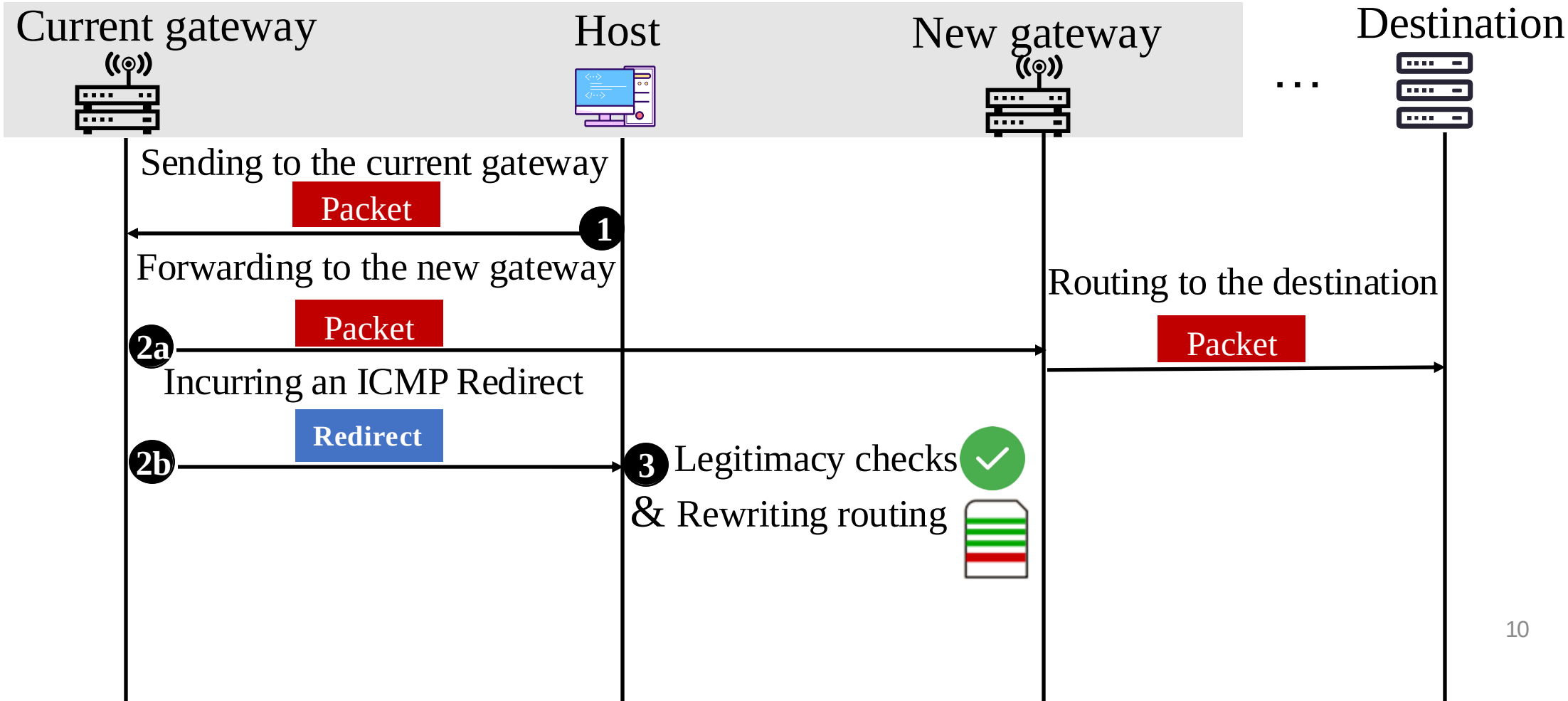
The Mechanism of ICMP Redirect

ICMP redirects help Host update its routing and optimize the forwarding path dynamically, thus improving the network performance.



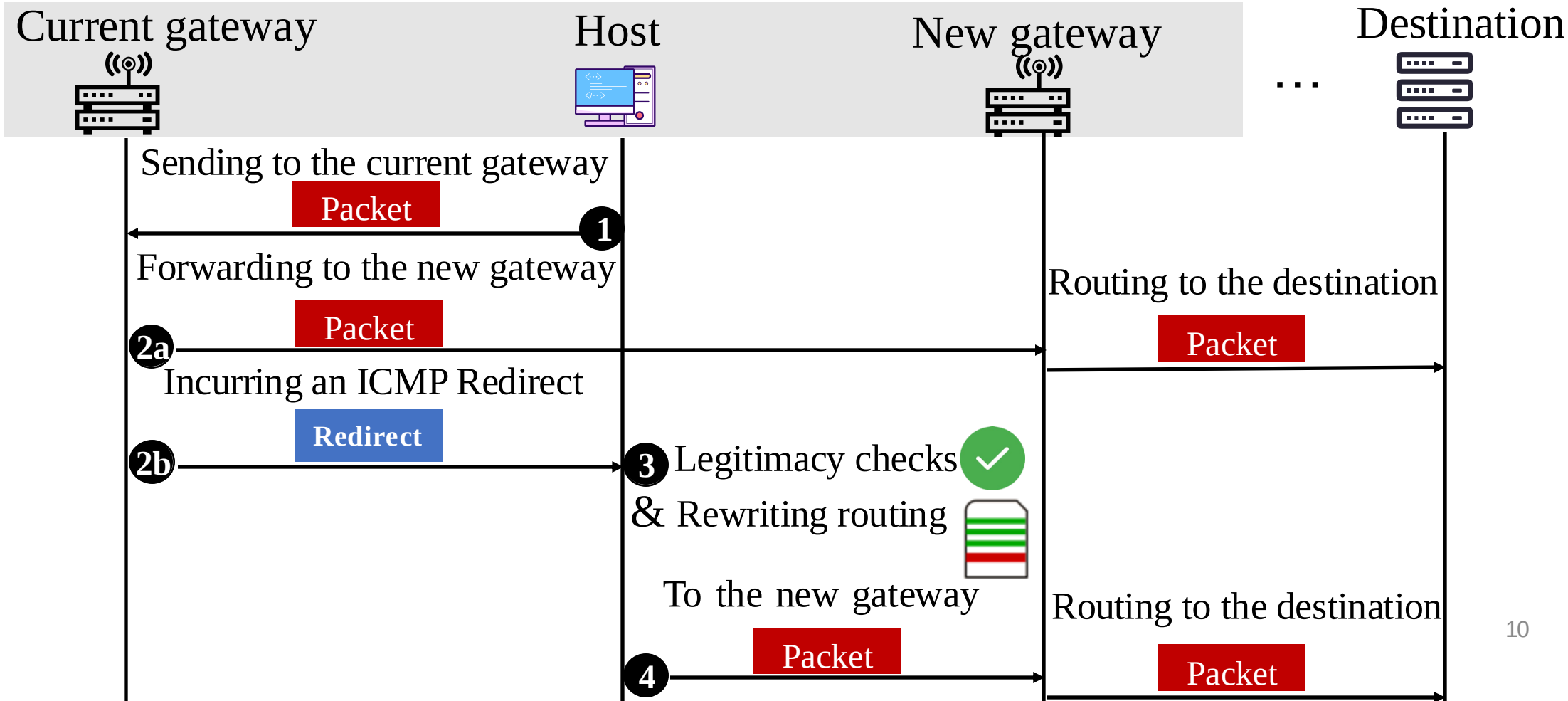
The Mechanism of ICMP Redirect

ICMP redirects help Host update its routing and optimize the forwarding path dynamically, thus improving the network performance.



The Mechanism of ICMP Redirect

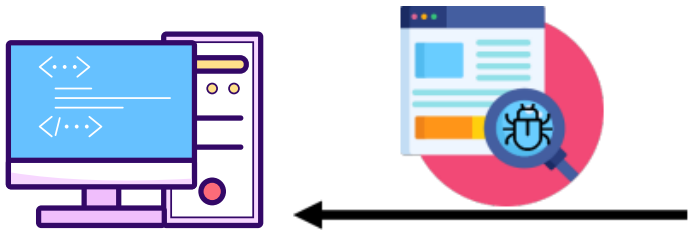
ICMP redirects help Host update its routing and optimize the forwarding path dynamically, thus improving the network performance.

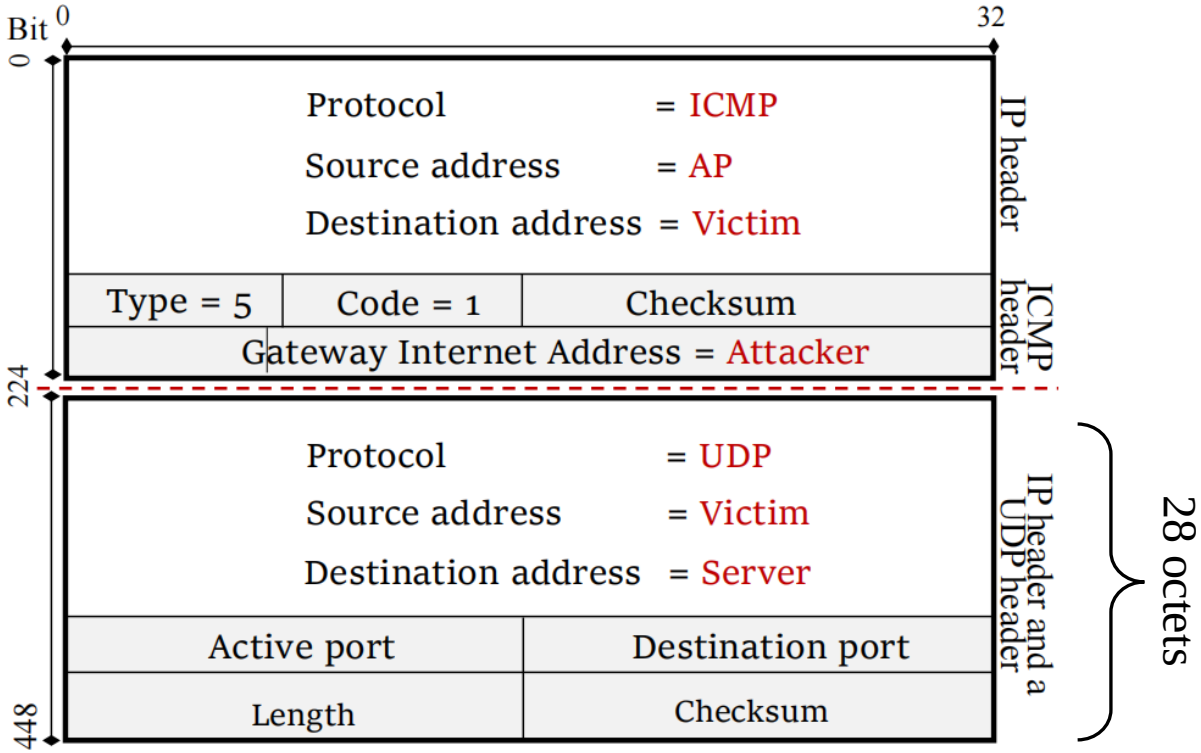


Legitimacy Checks over ICMP Redirects

Legitimacy Checks over ICMP Redirects

The host will perform **two checks** over the received ICMP redirects.

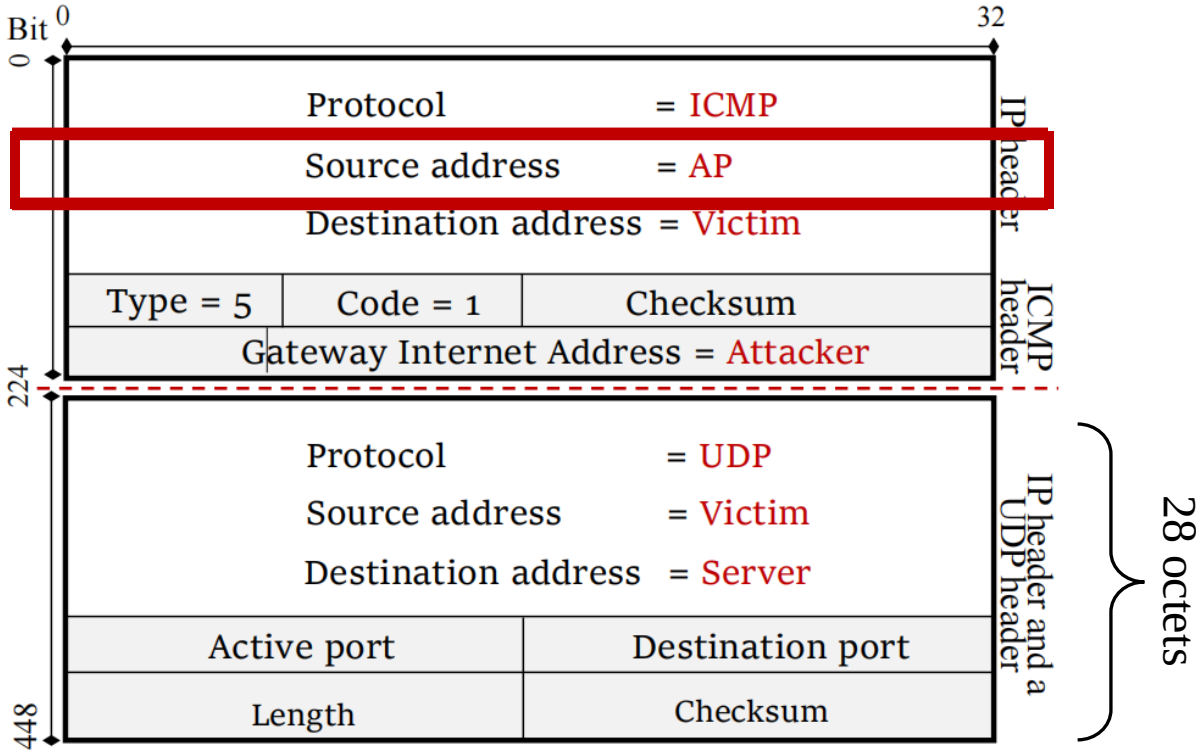




Legitimacy Checks over ICMP Redirects

The host will perform **two checks** over the received ICMP redirects.

(1) Whether the message was sent by its current gateway.

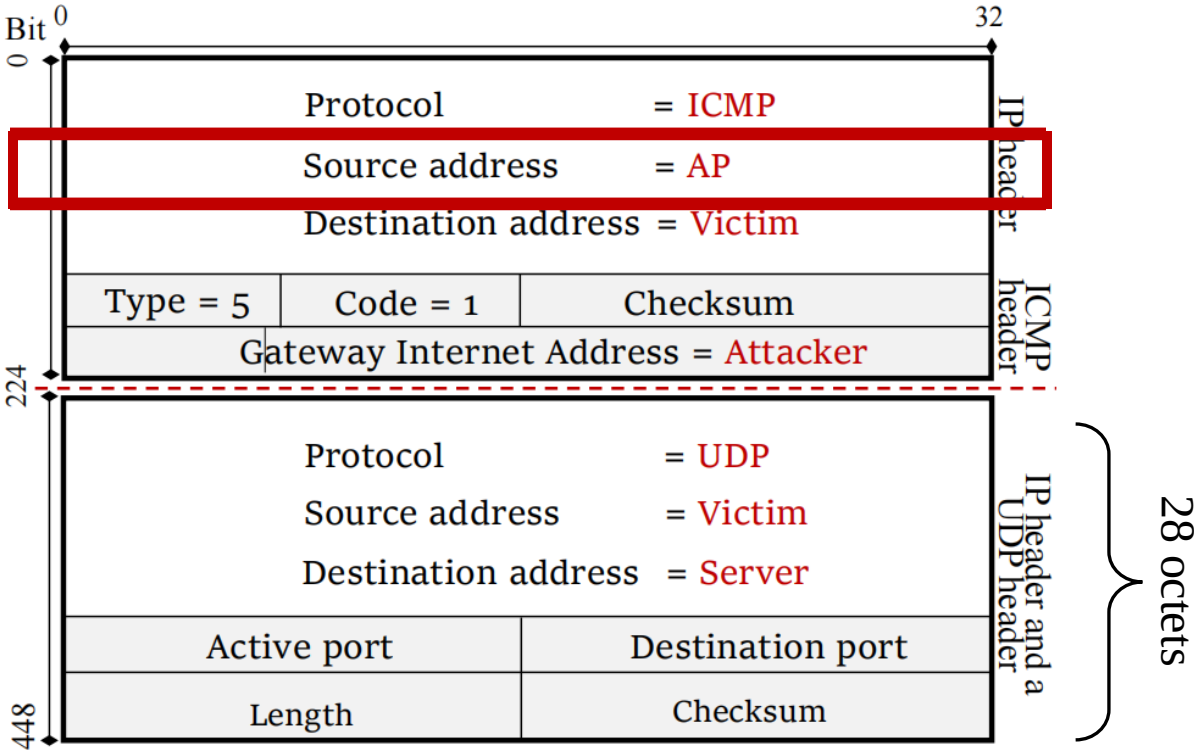


Legitimacy Checks over ICMP Redirects

The host will perform **two checks** over the received ICMP redirects.

(1) Whether the message was sent by its current gateway, i.e., the AP.

IP spoofing



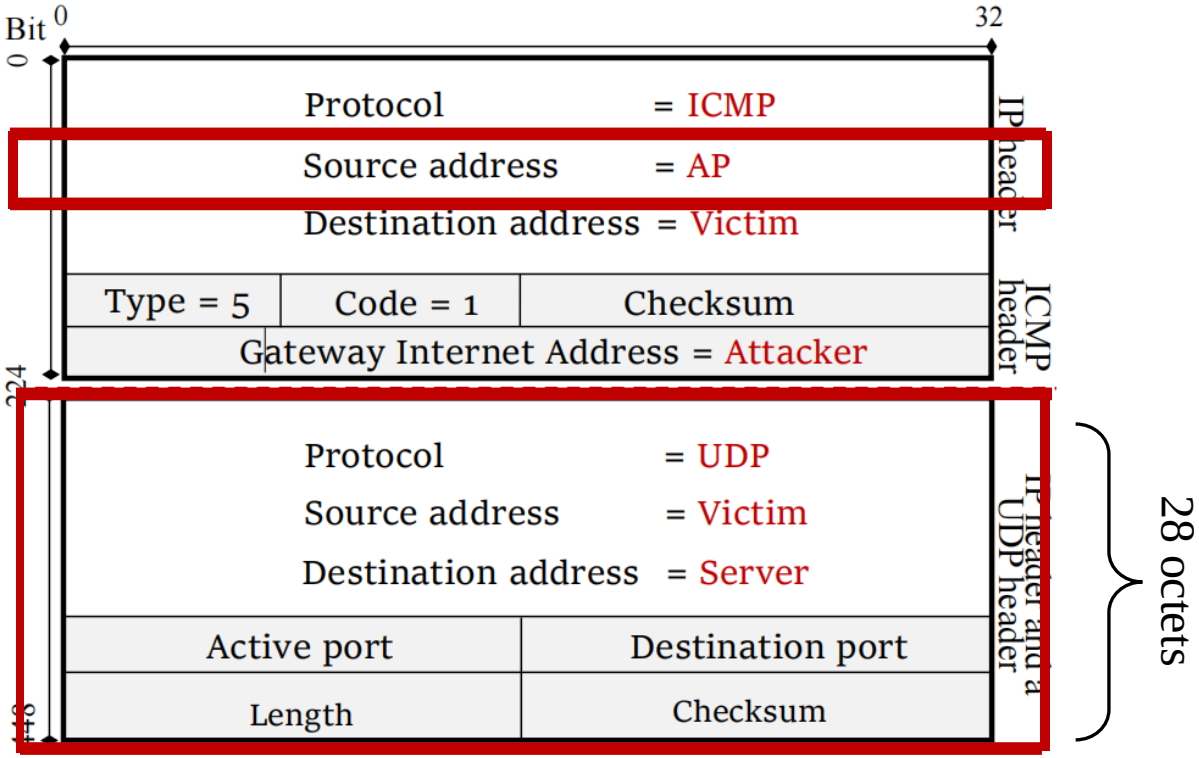
Legitimacy Checks over ICMP Redirects

The host will perform **two checks** over the received ICMP redirects.

(1) Whether the message was sent by its current gateway, i.e., the AP.

IP spoofing

(2) Checking at least 28 octets of the original packet that triggered the ICMP message.



Legitimacy Checks over ICMP Redirects

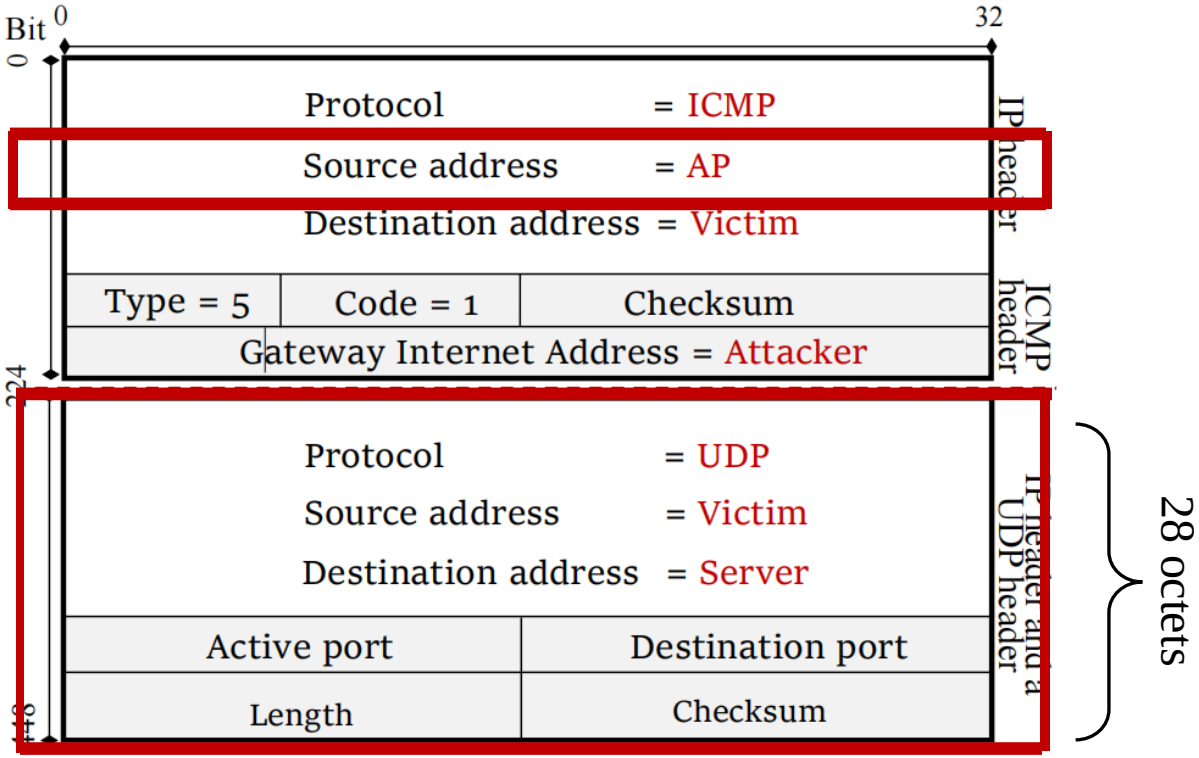
The host will perform **two checks** over the received ICMP redirects.

(1) Whether the message was sent by its current gateway, i.e., the AP.

IP spoofing

(2) Checking at least 28 octets of the original packet that triggered the ICMP message.

Crafting 28 octets data



Legitimacy Checks over ICMP Redirects

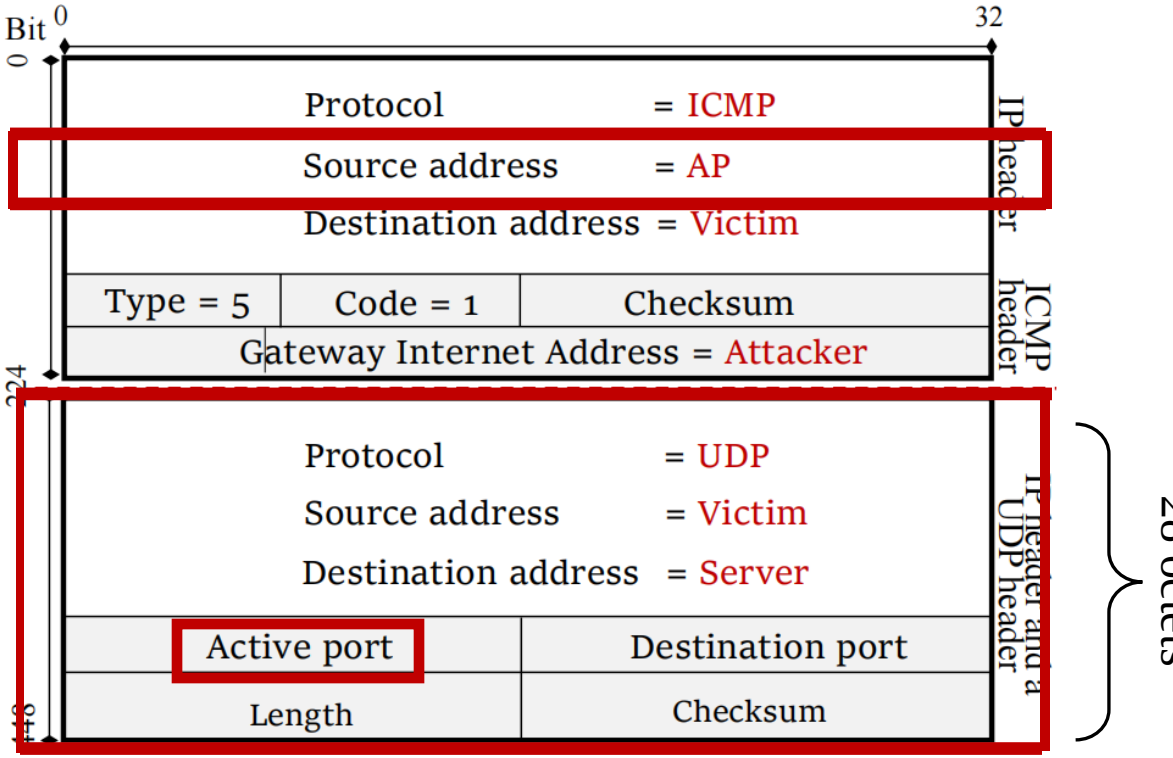
The host will perform **two checks** over the received ICMP redirects.

(1) Whether the message was sent by its current gateway, i.e., the AP.

IP spoofing

(2) Checking at least 28 octets of the original packet that triggered the ICMP message.

Crafting 28 octets data



- Stateless protocols (**e.g., UDP**) cannot remember the data that has been sent earlier.
- Attackers can craft ICMP redirects **embedded with stateless protocol data** to evade the checks (including the existence of the corresponding UDP socket).

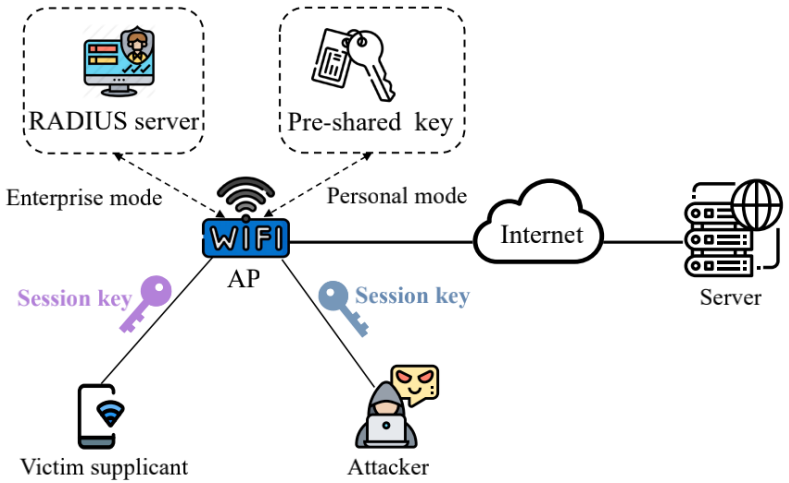
Traffic Hijacking in Wi-Fi Networks

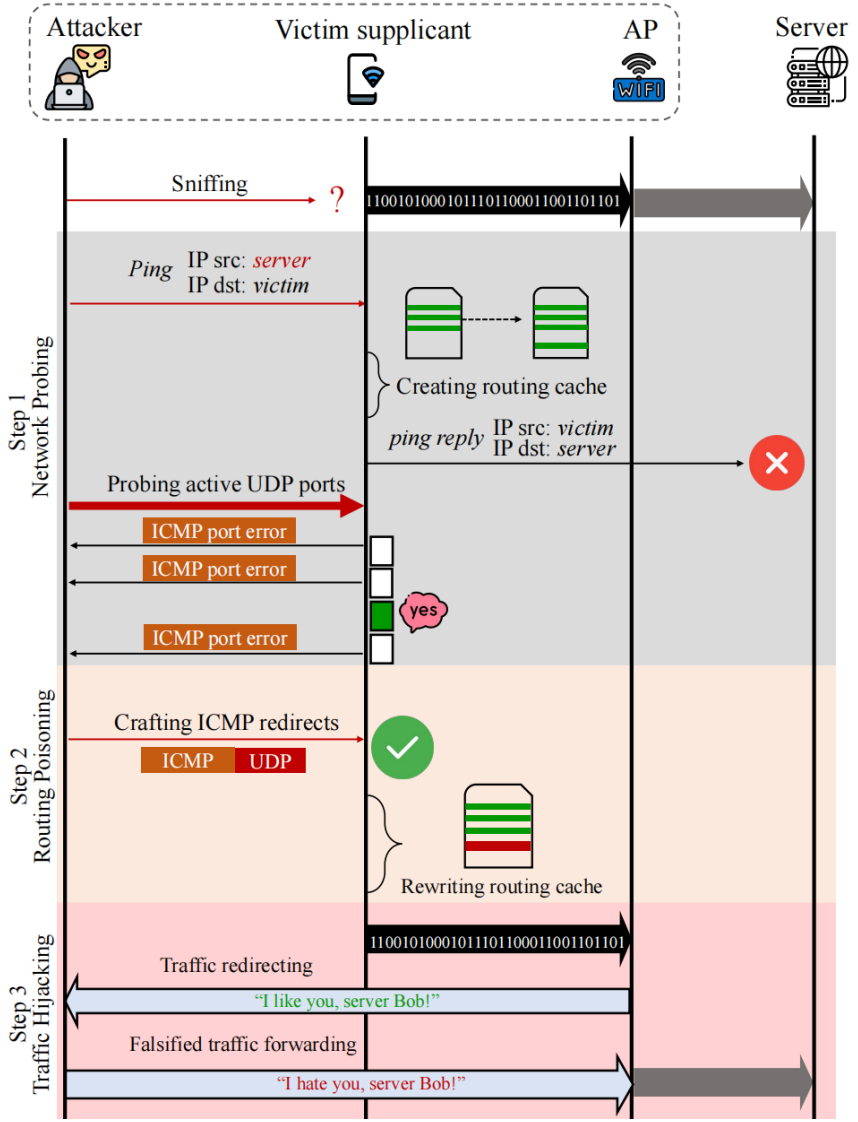
Traffic Hijacking in Wi-Fi Networks

Step 1: Network Probing

Step 2: Routing Poisoning

Step 3: Traffic Hijacking





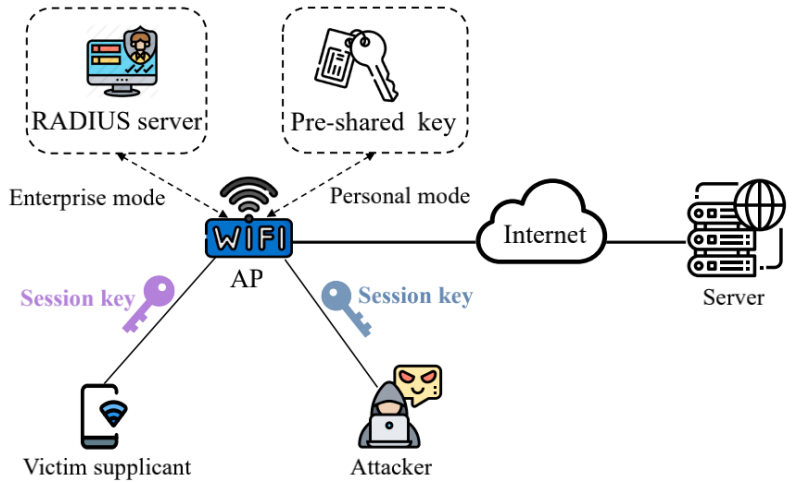
Traffic Hijacking in Wi-Fi Networks

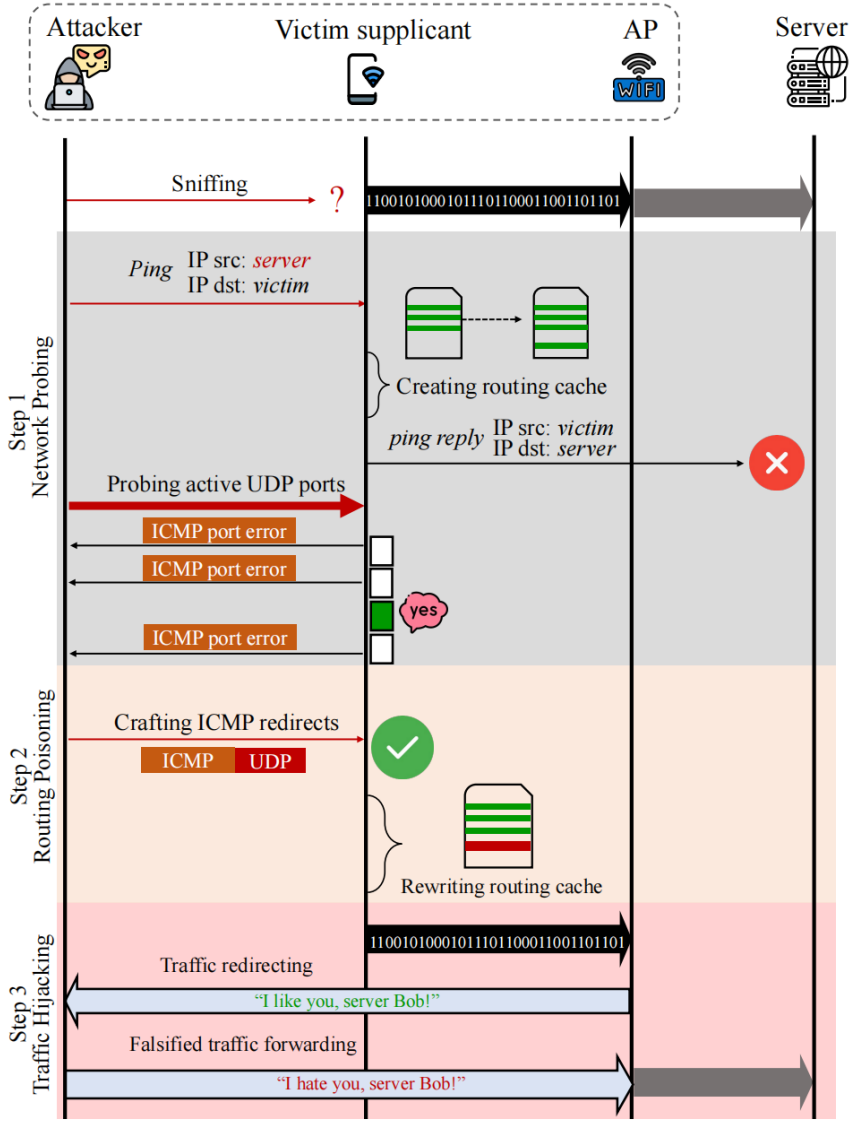
Step 1: Network Probing

- Creating routing cache via spoofed Ping

Step 2: Routing Poisoning

Step 3: Traffic Hijacking





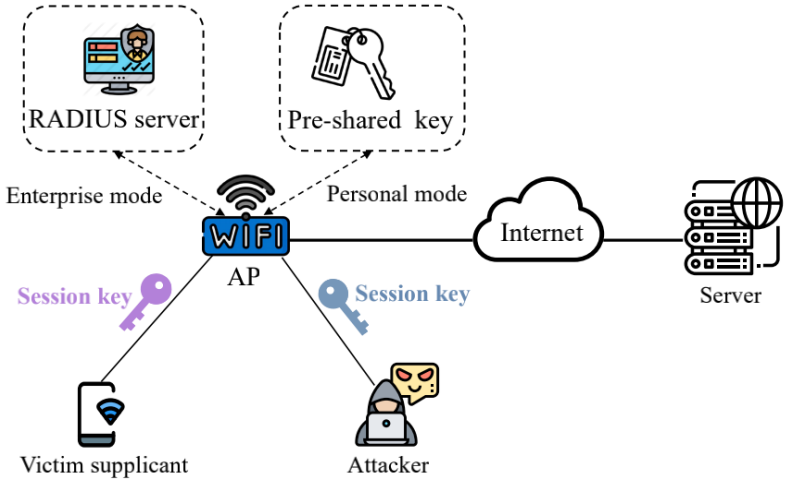
Traffic Hijacking in Wi-Fi Networks

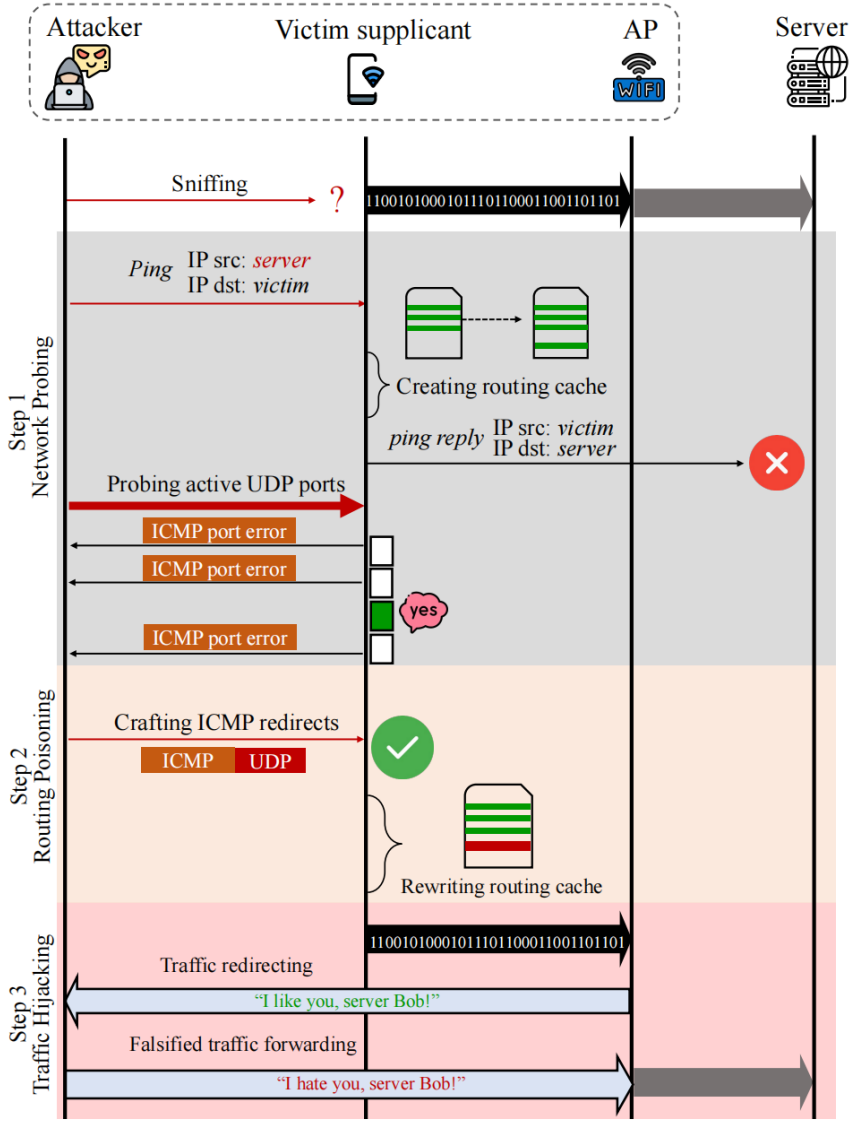
Step 1: Network Probing

- Creating routing cache via spoofed Ping
- Probing active UDP ports

Step 2: Routing Poisoning

Step 3: Traffic Hijacking





Traffic Hijacking in Wi-Fi Networks

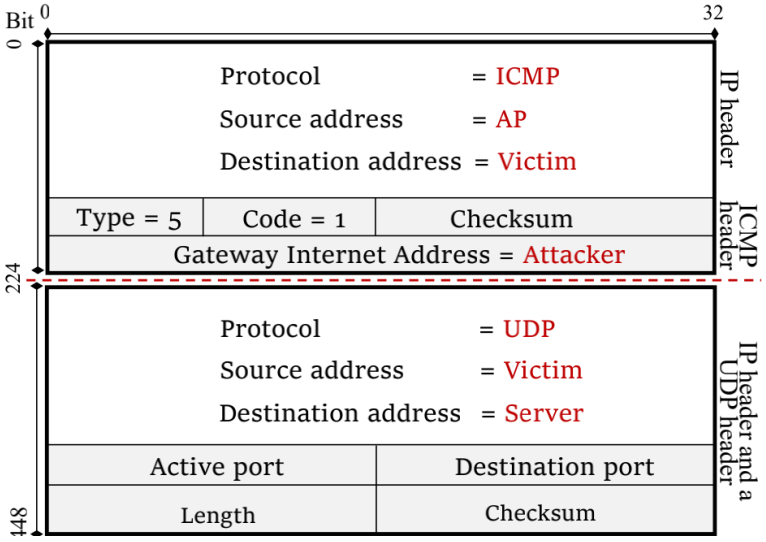
Step 1: Network Probing

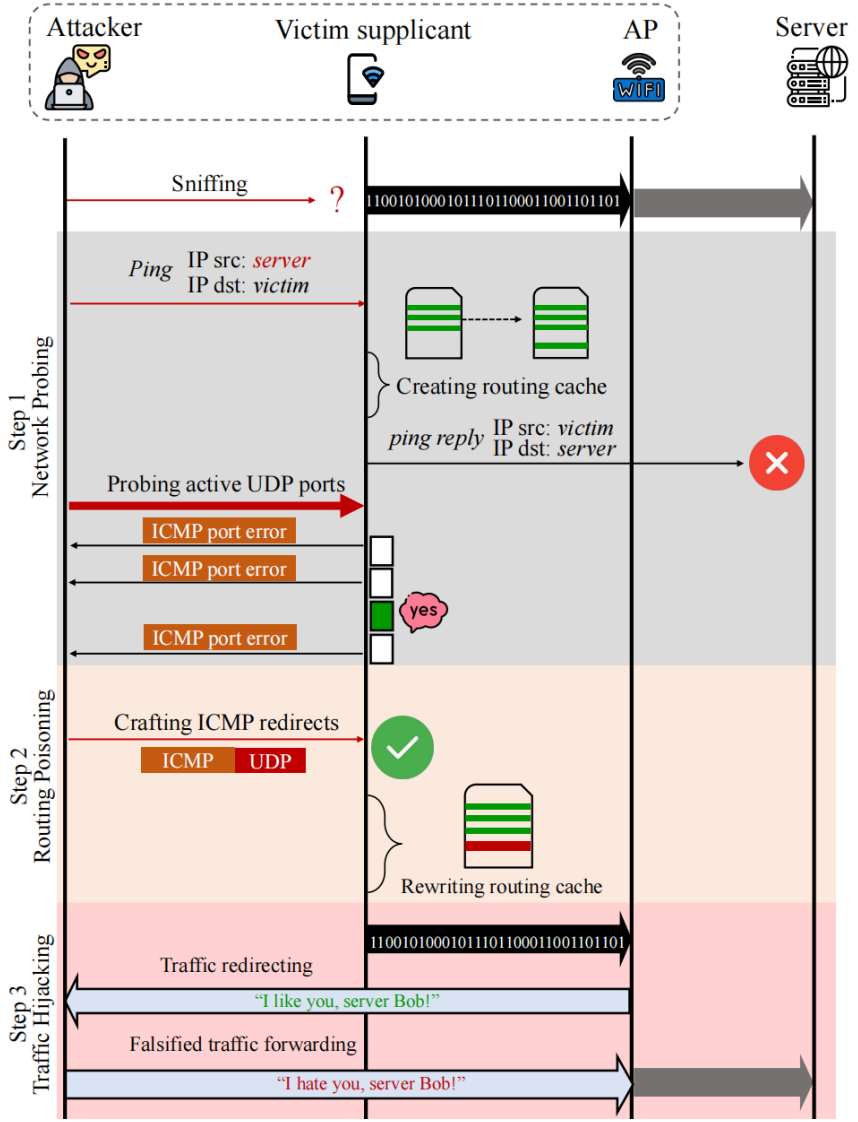
- Creating routing cache via spoofed Ping
- Probing active UDP ports

Step 2: Routing Poisoning

- Sending crafted ICMP redirects

Step 3: Traffic Hijacking





Traffic Hijacking in Wi-Fi Networks

Step 1: Network Probing

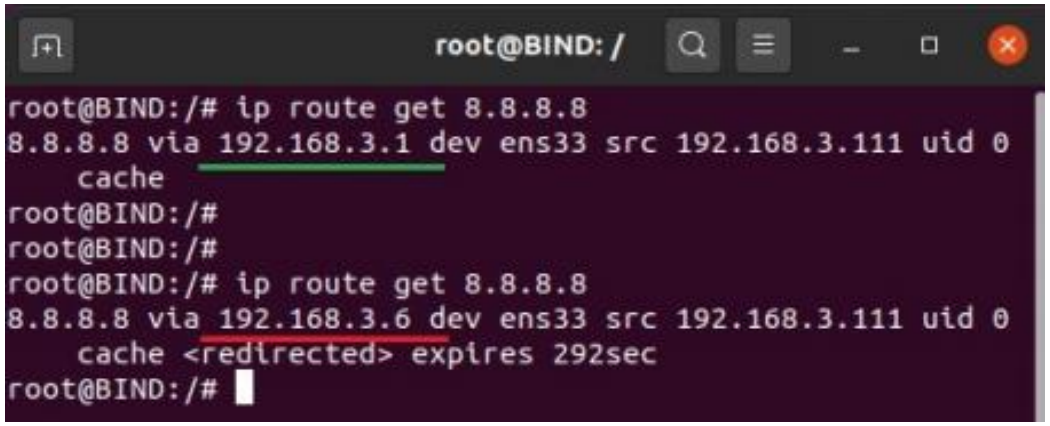
- Creating routing cache via spoofed Ping
- Probing active UDP ports

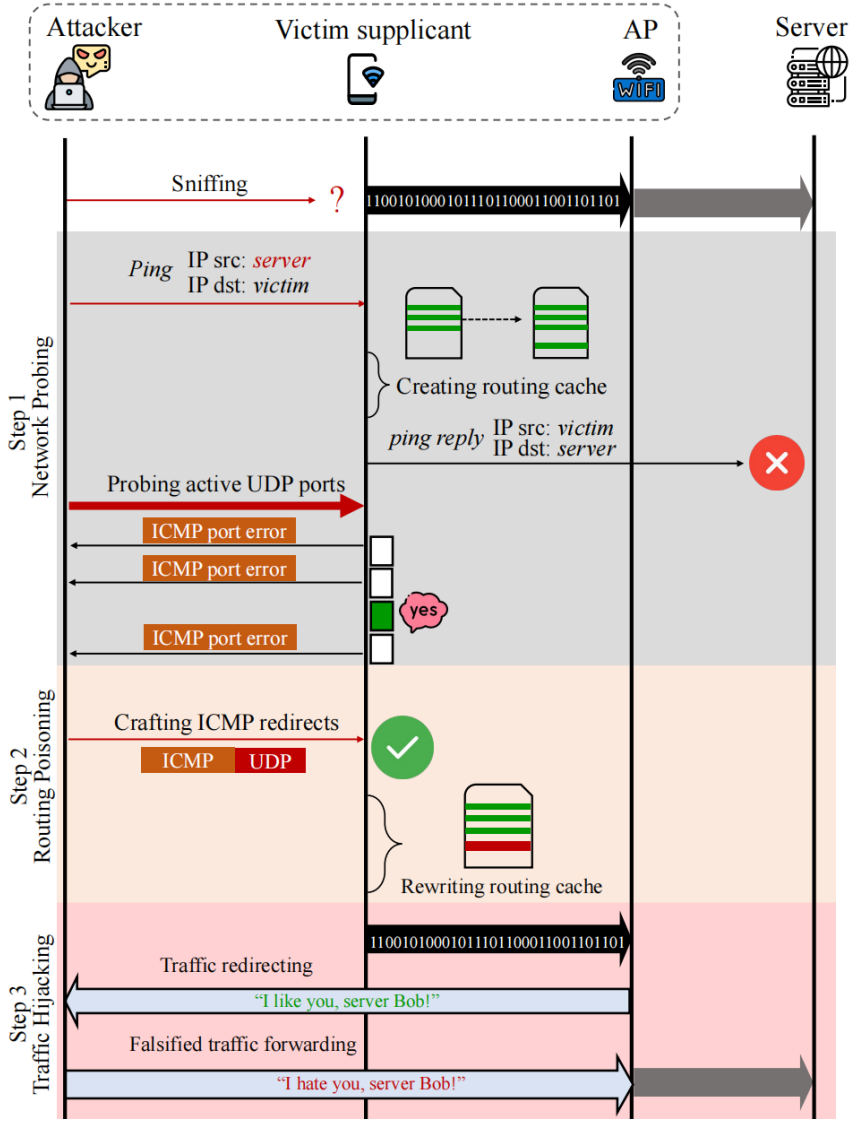
Step 2: Routing Poisoning

- Sending crafted ICMP redirects

Step 3: Traffic Hijacking

- Redirecting network traffic





Traffic Hijacking in Wi-Fi Networks

Step 1: Network Probing

- Creating routing cache via spoofed Ping
- Probing active UDP ports

Step 2: Routing Poisoning

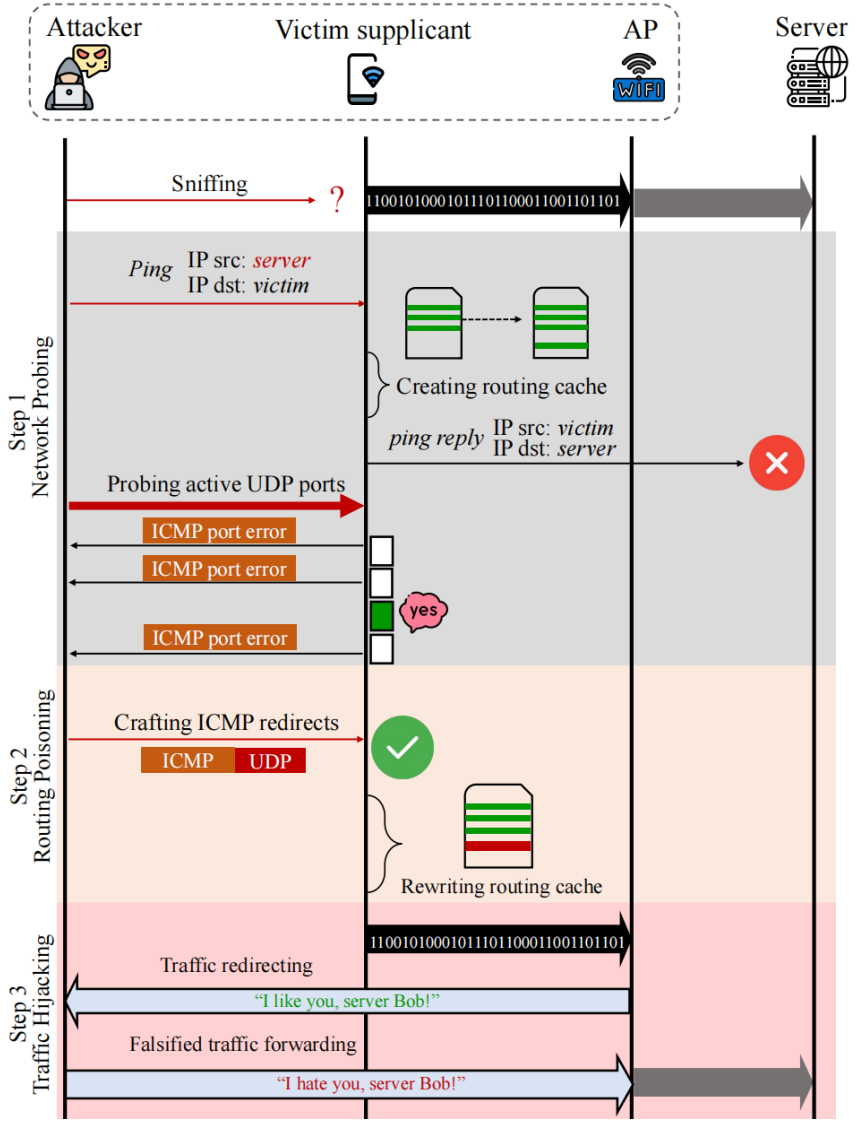
- Sending crafted ICMP redirects

Step 3: Traffic Hijacking

- Redirecting network traffic

Then the attack can be conducted under various scenarios to compromise the network.

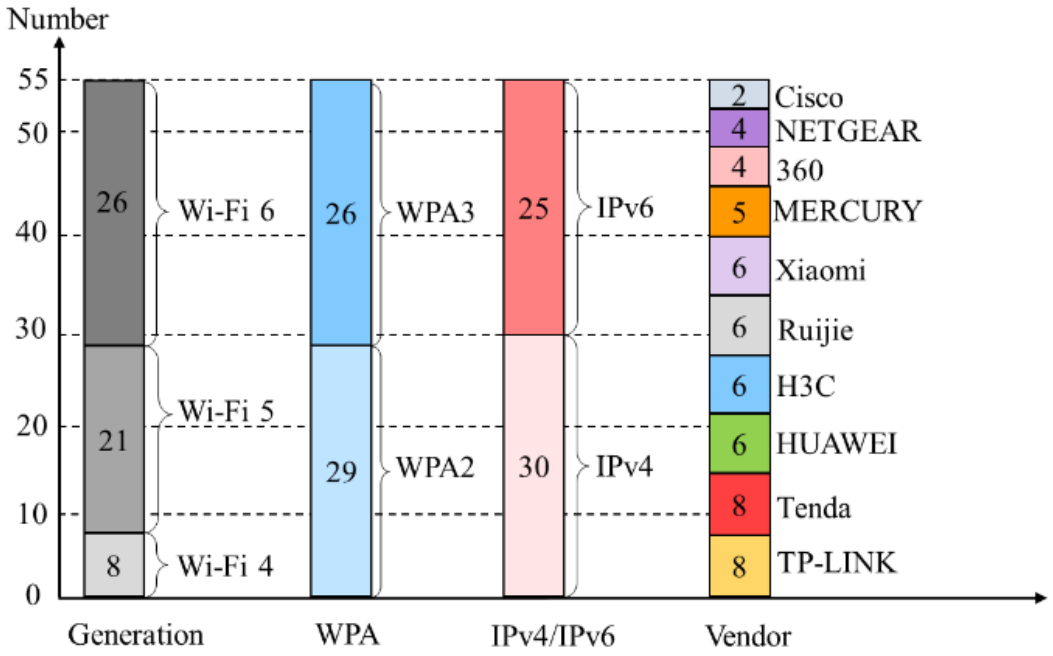
e.g., hijack DNS queries from the victim or steal personal privacy from HTTP traffic.



Empirical Study

Empirical Study

- NPU processor in AP routers has **design defects**, which makes AP routers not able to effectively identify and filter ICMP redirect messages forged by the attacker. (Qualcomm: CVE-2022-25667)
- Our evaluations against 55 mainstream wireless routers confirm the vulnerability. None of them can block the crafted ICMP redirect messages with the spoofed source IP address of the wireless router itself.



Statistics of the 55 vulnerable wireless routers.

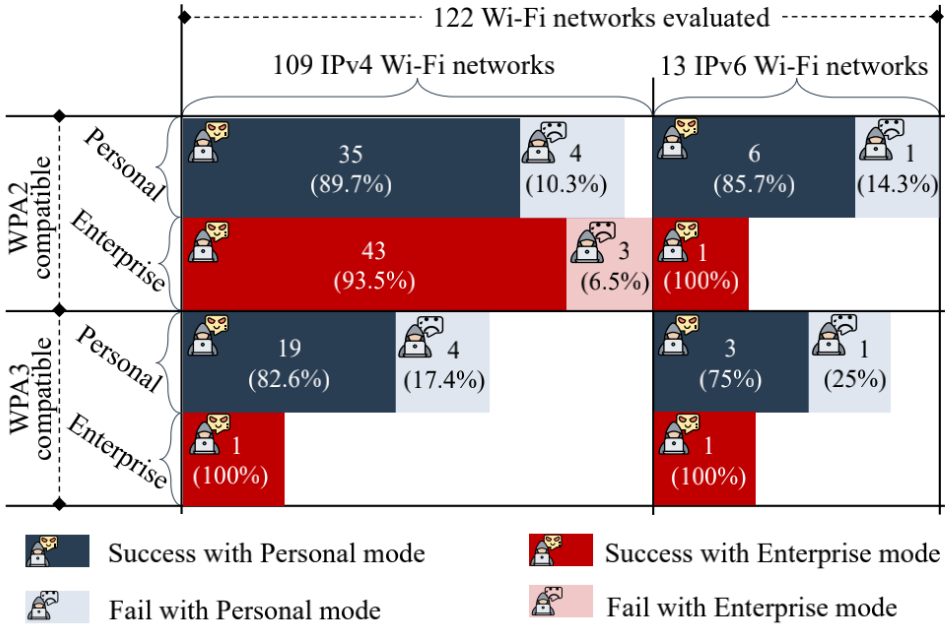
Wi-Fi router	Generation	WPA	Vendor	IPv6 Enabled	Security Metrics: MAC-ADDR Filtering	Anti-Flooding	Suspicious Packets Blocking
TL-XVR1800L	Wi-Fi 6	WPA3	TP-LINK	Yes	●	●	○
TL-XDR1860	Wi-Fi 6	WPA3	TP-LINK	Yes	●	○	○
TL-WAR1200L	Wi-Fi 5	WPA2	TP-LINK	Yes	●	●	●
TL-WDR7660	Wi-Fi 5	WPA2	TP-LINK	No	○	●	●
TL-WR845N	Wi-Fi 4	WPA2	TP-LINK	No	○	○	●
WAP150	Wi-Fi 5	WPA2	Cisco	Yes	●	●	●
WAP125	Wi-Fi 5	WPA2	Cisco	Yes	●	○	●
Ax12	Wi-Fi 6	WPA3	Tenda	Yes	●	●	●
AC23	Wi-Fi 5	WPA2	Tenda	Yes	●	●	○
AC11	Wi-Fi 5	WPA2	Tenda	No	●	○	○
AC10	Wi-Fi 5	WPA2	Tenda	Yes	●	●	●
AX3pro	Wi-Fi 6	WPA3	HUAWEI	Yes	●	●	●
AX2pro	Wi-Fi 6	WPA3	HUAWEI	Yes	●	○	●
WS5281	Wi-Fi 5	WPA2	HUAWEI	Yes	●	●	○
WS5102	Wi-Fi 5	WPA2	HUAWEI	Yes	●	○	○
V6G	Wi-Fi 6	WPA3	360	Yes	●	●	●
5Pro	Wi-Fi 5	WPA2	360	Yes	●	●	○
360mini	Wi-Fi 4	WPA2	360	No	○	●	○
GR-5400AX	Wi-Fi 6	WPA3	H3C	No	●	●	●
N21	Wi-Fi 5	WPA2	H3C	No	●	○	○
ER-8300G2	Wi-Fi 4	WPA2	H3C	No	●	●	○
RG-EW1800GX PRO	Wi-Fi 6	WPA3	Ruijie	No	●	○	●
RG-EW1200G PRO	Wi-Fi 5	WPA2	Ruijie	Yes	●	○	○
RG-EW1200 PRO	Wi-Fi 5	WPA2	Ruijie	No	●	○	○
Redmi AX9000	Wi-Fi 6	WPA3	Xiaomi	Yes	●	●	●
Redmi AX5 RA67	Wi-Fi 6	WPA3	Xiaomi	Yes	●	●	○
Mi 4C	Wi-Fi 4	WPA2	Xiaomi	No	●	○	○
X18G	Wi-Fi 6	WPA3	MERCURY	Yes	●	●	●
D121	Wi-Fi 5	WPA2	MERCURY	Yes	●	●	●
MW325R	Wi-Fi 4	WPA2	MERCURY	No	●	○	○
RAX50	Wi-Fi 6	WPA3	NETGEAR	Yes	●	●	●
RAX20	Wi-Fi 6	WPA3	NETGEAR	Yes	●	●	○

○ means that the security metric is supported by the router, and ● means that the security metric is not supported.

Vulnerable Wireless Routers Allowing Crafted ICMP Redirect To Pass Through

Empirical Study

- We perform the attack in 122 real-world Wi-Fi networks, including various real-world public Wi-Fi networks secured by WPA2 or WPA3.
- Attack success rate is higher than 89%, i.e., totally 109 of the 122 Wi-Fi networks. Failure cases are mainly due to specific network policies such as AP Isolation.



Attacks evaluation based on 122 real-world Wi-Fi networks

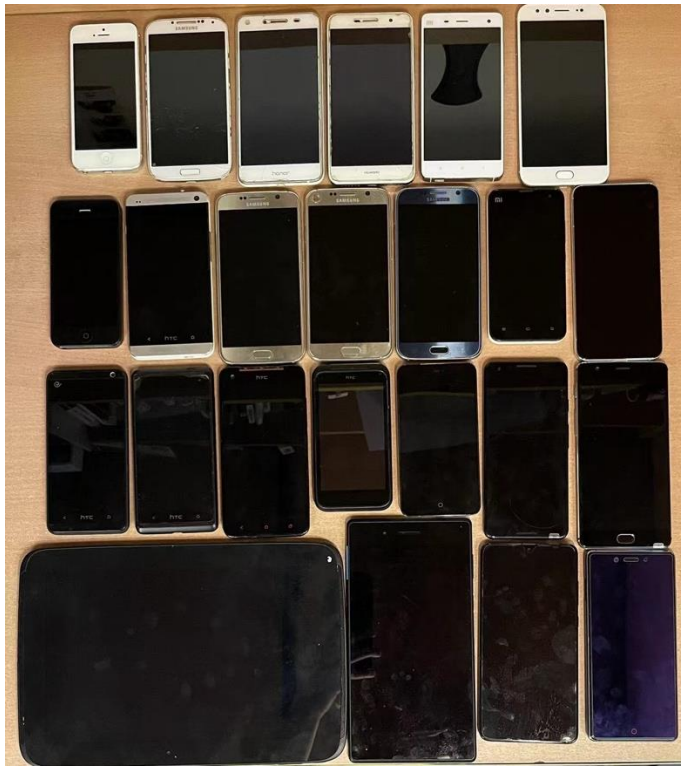
No.	SSID	AP vendor	IPv4/IPv6	Wi-Fi generation	WPA2/3 Enterprise/Personal	Success rate
1	Restaurant 1	Abloomy	◐	Wi-Fi 4	WPA2-Enterprise	46/50
2	Restaurant 2	TP-LINK	◐	Wi-Fi 5	WPA2-Enterprise	42/50
3	Restaurant 3	H3C	◐	Wi-Fi 4	WPA2-Personal	45/50
4	Campus 1	TP-LINK	●	Wi-Fi 5	WPA2-Enterprise	47/50
5	Campus 2	H3C	◐	Wi-Fi 5	WPA2-Enterprise	49/50
6	Campus 3	iKuai	◐	Wi-Fi 4	WPA2-Personal	44/50
7	Fast food restaurant 1	WiMaster	◐	Wi-Fi 5	WPA2-Enterprise	47/50
8	Fast food restaurant 2	Abloomy	◐	Wi-Fi 4	WPA2-Enterprise	44/50
9	Fast food restaurant 3	WiMaster-Mini	◐	Wi-Fi 5	WPA2-Enterprise	46/50
10	Coffee shop 1	WiMaster	◐	Wi-Fi 4	WPA2-Enterprise	49/50
11	Coffee shop 2	TP-LINK	◐	Wi-Fi 4	WPA2-Enterprise	47/50
12	Coffee shop 3	TP-LINK	◐	Wi-Fi 5	WPA2-Personal	49/50
13	Shopping mall 1	HUAWEI	◐	Wi-Fi 5	WPA2-Enterprise	45/50
14	Shopping mall 2	TP-LINK	◐	Wi-Fi 4	WPA2-Enterprise	46/50
15	Shopping mall 3	Tenda	◐	Wi-Fi 5	WPA2-Enterprise	44/50
16	Bookstore 1	360	◐	Wi-Fi 4	WPA2-Enterprise	44/50
17	Bookstore 2	Xiaomi	◐	Wi-Fi 6	WPA3-Personal	47/50
18	Bookstore 3	H3C	◐	Wi-Fi 6	WPA3-Personal	48/50
19	Office building 1	TP-LINK	◐	Wi-Fi 5	WPA2-Enterprise	46/50
20	Office building 2	Tenda	◐	Wi-Fi 5	WPA2-Enterprise	45/50
21	Office building 3	TP-LINK	●	Wi-Fi 6	WPA3-Personal	46/50
22	Experience store 1	Xiaomi	◐	Wi-Fi 6	WPA3-Personal	45/50
23	Experience store 2	H3C	●	Wi-Fi 5	WPA2-Personal	47/50
24	Experience store 3	Xiaomi	◐	Wi-Fi 5	WPA2-Personal	47/50
25	Cinema 1	Xiaomi	◐	Wi-Fi 5	WPA2-Enterprise	48/50
26	Cinema 2	HUAWEI	◐	Wi-Fi 6	WPA2-Enterprise	49/50
27	Hotel 1	Gee	◐	Wi-Fi 5	WPA2-Enterprise	48/50
28	Hotel 2	ZH-A0101	◐	Wi-Fi 4	WPA2-Enterprise	43/50
29	Enterprise 1	TP-LINK	◐	Wi-Fi 6	WPA3-Enterprise	46/50
30	Enterprise 2	TP-LINK	●	Wi-Fi 6	WPA3-Enterprise	44/50

Experimental Results of Traffic Hijacking in 30 Wi-Fi Networks.

Empirical Study

Device	Android version	Device	Android version
HTC-S710e	2.2.1	HTC-X920e	4.1.1
HTC-609d	4.1.2	HTC-802t	4.4.2
Meizu-M040	4.4.4	Galaxy S4	5.0.1
Nexus 10	5.1	HUAWEI Honor 5	5.1
HUAWEI 5A	5.1	Xiaomi Mi 4	6.0.1
Galaxy S6	6.0.1	Lenovo Tab S6000	7.0
OnePlus 3	7.1.1	Xiaomi Mi 4	7.1.1
Xiaomi Mi 4	8.0.0	Nubia Z11	8.0.0
OnePlus 3	8.0.1	vivo X9s	8.1.0
Nexus 10	8.1.0	Xiaomi Mi 4	9.0
Galaxy S6	9.0	Pixel 3	9.0

Affected Android Devices in Our Tests.



- The ICMP redirect mechanism is enabled by default in a wide range of OSes, e.g., Linux 2.6.39 and beyond, FreeBSD 6.0 and beyond, Mac OS 10.0.4~10.10.5, iOS 1~8, and Android kernel version before 10.0 (more than 40%).

Countermeasures

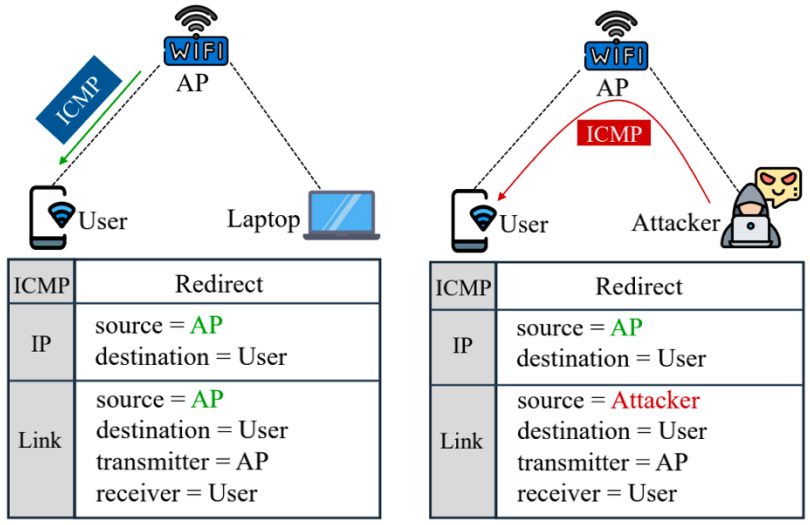
Countermeasures

Enhancing Clients to Check Cross-Layer Interactions

- detect inconsistency between the source IP address and the source MAC address of ICMP redirects

Enhancing APs to Throttle Crafted ICMP Redirects

- identify crafted ICMP redirects whose source IP address is specified as the AP's IP address during the message forwarding.



(a) Legitimate ICMP redirect message issued from the AP. (b) Illegitimate ICMP redirect message crafted by an attacker.

Conclusion

- We uncover a vulnerability of the NPUs in AP routers that can be exploited by a malicious supplicant to spoof the legitimate AP to forge ICMP error messages in Wi-Fi networks.
- We develop a new technique to evade the legitimacy checks on the ICMP redirect messages. And we demonstrate that ICMP redirects can be exploited to evade security features (even WPA3) of Wi-Fi networks to perform a MITM attack.
- We evaluate the attack against popular routers and real Wi-Fi networks. And we propose two countermeasures via enhancing the Clients or the APs.

Thank you!